UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/492,454	01/27/2000	Xiaowen Yang	YANG 1	9889

7590 08/11/2008

William H Bollman
MANELLI DENISON & SELTER PLLC
2000 M Street NW
Suite 700
Washington, DC 20036-3307

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
08/11/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/492,454	YANG, XIAOWEN	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-8 and 10-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-8 and 10-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 January 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the RCE filed on 30 May 2008.

2. Claims 1, 3-8 and 10-22 are pending in the application.

3. Claims 1, 3-8 and 10-22 have been rejected.

4. Claims 2 and 9 have been cancelled.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 30 May 2008 has been entered.

Response to Arguments

6. Applicant's arguments with respect to claims 1, 3-8 and 10-22 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 3-8 and 10-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hamada U.S. Patent No. 6,754,347 BI in view of Norr U.S. Patent No. 7,085,377 B1.

As to claim 1, Hamada discloses a device to descramble a packetized digital data stream, comprising:

a receiver to receive a digital data stream comprising a plurality of data packets (i.e. Receiver 14 receives the dynamically encrypted stream of data at a data demultiplexer 30, which again assumes that the encryption key or encryption parameters have been multiplexed into the stream. Output from demultiplexer 30 is the encryption key and/or parameters, as well as the encrypted MPEG stream. This data is forwarded to a decryption unit 32 which then decrypts the data using the encryption information and provides an unencrypted MPEG stream to a conventional MPEG decoder 34.) [column 6 line 66 to column 7 line 7]; and

a descrambler to descramble (i.e. Receiver 14 receives the dynamically encrypted stream of data at a data demultiplexer 30, which again assumes that the encryption key or encryption parameters have been multiplexed into the stream. Output from demultiplexer 30 is the encryption key and/or parameters, as well as the encrypted MPEG stream. This data is forwarded to a decryption unit 32 which

then decrypts the data using the encryption information and provides an unencrypted MPEG stream to a conventional MPEG decoder 34.) [column 6 line 66 to column 7 line 7] the partially scrambled data payload (i.e. These parameters imply the following. The unit which will be encrypted is the picture slice. One fourth of the slices (256/1024) (i.e., every fourth slice) will be encrypted. Further, the first slice will be unencrypted; encryption will begin with the second slice (delay of 1) and continue with every fourth slice thereafter. The encryption key, after having been initialized, will be updated at the start of every sixteenth picture (key update frequency).) [column 6, lines 18-24];

wherein the partially scrambled data payload is comprised of a scrambled portion surrounded on both sides by an unscrambled portion (i.e. Sender 12 includes an encryption unit 20 which (in this example) receives as inputs an encryption key from a dynamic key generator 22, and the unencrypted, but encoded MPEG data stream. Any conventional encryption technique can be employed within encryption unit 20, provided that the encryption can be modified dynamically as presented herein by changing an encryption key or one or more other encryption parameters as discussed above. Output from encryption unit 20 is an encrypted MPEG stream. In this example, the encrypted MPEG stream is fed to a data multiplexer 24 which multiplexes into the stream the encryption key employed to encrypt the stream and the encryption parameters employed by the encryption unit. Data multiplexer 24 is optional since the

> encryption key and encryption parameters could be forwarded independent from the encrypted stream of data, for example, on a dedicated line (not shown) to the receiver 14.) [column 6, lines 49-65].

Hamada does not teach a receiver to receive a packet of a single digital data stream wherein only some of a plurality of data packets within the single digital data stream are scrambled.

Norr teaches selectively encrypting some of the packets [column 4, lines 29-62].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hamada so that the packets containing the premium channels would have only been encrypted. The packets would have included a header portion and a data payload. The data payload would have included a scrambled central portion and an unscrambled portion. A descrambler would have descrambled the scrambled central portion of the data payload of the packet. The header portion would have been entirely unscrambled.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hamada by the teaching of Norr because it helps avoid unnecessary downloading of information already transmitted via broadcast airwaves, while also ensuring that copyright owners and service providers receive appropriate payments [column 2, lines 40-49].

As to claims 3, 11, 16, 18, 20 and 22, Hamada teaches that the digital data stream is an MPEG-2 digital data stream [column 7, lines 28-33].

As to claim 4, Hamada teaches that the packet contains compressed digital data (i.e. MPEG is compressed data) [column 7, lines 28-33].

As to claim 5, Hamada teaches that the compressed digital data includes a video signal [column 5, lines 4-8].

As to claim 6, Hamada teaches that the compressed digital data includes an audio signal [column 5, lines 4-8].

As to claim 7, Hamada teaches that the compressed digital data includes a video signal and an audio signal [column 5, lines 4-8].

As to claim 8, Hamada teaches a method of scrambling a packetized digital data stream, comprising;

> producing a single data packet stream comprising a plurality of data packets (i.e. Receiver 14 receives the dynamically encrypted stream of data at a data demultiplexer 30, which again assumes that the encryption key or encryption parameters have been multiplexed into the stream. Output from demultiplexer 30 is the encryption key and/or parameters, as well as the encrypted MPEG stream. This data is forwarded to a decryption unit 32 which then decrypts the data using the encryption information and provides an unencrypted MPEG stream to a conventional MPEG decoder 34.) [column 6 line 66 to column 7 line 7]; and
>
> scrambling a central portion of a data payload (i.e. These parameters imply the following. The unit which will be encrypted is the picture slice. One fourth of the slices (256/1024) (i.e., every fourth slice) will be encrypted. Further, the first slice will be unencrypted; encryption will begin with the second slice

(delay of 1) and continue with every fourth slice thereafter. The encryption key, after having been initialized, will be updated at the start of every sixteenth picture (key update frequency).) [column 6, lines 18-24];

wherein the partially scrambled data payload is comprised of the scrambled central portion (i.e. Sender 12 includes an encryption unit 20 which (in this example) receives as inputs an encryption key from a dynamic key generator 22, and the unencrypted, but encoded MPEG data stream. Any conventional encryption technique can be employed within encryption unit 20, provided that the encryption can be modified dynamically as presented herein by changing an encryption key or one or more other encryption parameters as discussed above. Output from encryption unit 20 is an encrypted MPEG stream. In this example, the encrypted MPEG stream is fed to a data multiplexer 24 which multiplexes into the stream the encryption key employed to encrypt the stream and the encryption parameters employed by the encryption unit. Data multiplexer 24 is optional since the encryption key and encryption parameters could be forwarded independent from the encrypted stream of data, for example, on a dedicated line (not shown) to the receiver 14.) [column 6, lines 49-65].

Hamada does not teach a receiver to receive a packet of a digital data stream wherein only some of a plurality of data packets within the digital data stream are scrambled.

Norr teaches selectively encrypting some of the packets [column 4, lines 29-62].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hamada so that the packets containing the premium channels would have only been encrypted. The packets would have included a header portion and a data payload. The data payload would have included a scrambled central portion and an unscrambled portion. A descrambler would have descrambled the scrambled central portion of the data payload of the packet. The header portion would have been entirely unscrambled.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hamada by the teaching of Norr because it helps avoid unnecessary downloading of information already transmitted via broadcast airwaves, while also ensuring that copyright owners and service providers receive appropriate payments [column 2, lines 40-49].

As to claim 10, Hamada teaches a method of scrambling a packetized digital data stream, comprising:

> producing a data packet stream comprising a plurality of data packets (i.e. Receiver 14 receives the dynamically encrypted stream of data at a data demultiplexer 30, which again assumes that the encryption key or encryption parameters have been multiplexed into the stream. Output from demultiplexer 30 is the encryption key and/or parameters, as well as the encrypted MPEG stream. This data is forwarded to a decryption unit 32 which then decrypts the data using the encryption information and provides an unencrypted MPEG stream to a conventional MPEG decoder 34.) [column 6 line 66 to column 7 line 7]; and

scrambling a central portion of a data payload to produce a partially scrambled data payload (i.e. These parameters imply the following. The unit which will be encrypted is the picture slice. One fourth of the slices (256/1024) (i.e., every fourth slice) will be encrypted. Further, the first slice will be unencrypted; encryption will begin with the second slice (delay of 1) and continue with every fourth slice thereafter. The encryption key, after having been initialized, will be updated at the start of every sixteenth picture (key update frequency).) [column 6, lines 18-24];

wherein the partially scrambled data payload is comprised of the scrambled central portion surround on both sides by an unscrambled portion (i.e. Sender 12 includes an encryption unit 20 which (in this example) receives as inputs an encryption key from a dynamic key generator 22, and the unencrypted, but encoded MPEG data stream. Any conventional encryption technique can be employed within encryption unit 20, provided that the encryption can be modified dynamically as presented herein by changing an encryption key or one or more other encryption parameters as discussed above. Output from encryption unit 20 is an encrypted MPEG stream. In this example, the encrypted MPEG stream is fed to a data multiplexer 24 which multiplexes into the stream the encryption key employed to encrypt the stream and the encryption parameters employed by the encryption unit. Data multiplexer 24 is optional since the encryption key and encryption parameters could be

forwarded independent from the encrypted stream of data, for example, on a dedicated line (not shown) to the receiver 14.) [column 6, lines 49-65].

Hamada does not teach a receiver to receive a packet of a digital data stream wherein only some of a plurality of data packets within the digital data stream are scrambled.

Norr teaches selectively encrypting some of the packets [column 4, lines 29-62].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hamada so that the packets containing the premium channels would have only been encrypted. The packets would have included a header portion and a data payload. The data payload would have included a scrambled central portion and an unscrambled portion. A descrambler would have descrambled the scrambled central portion of the data payload of the packet. The header portion would have been entirely unscrambled.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hamada by the teaching of Norr because it helps avoid unnecessary downloading of information already transmitted via broadcast airwaves, while also ensuring that copyright owners and service providers receive appropriate payments [column 2, lines 40-49].

As to claim 12, Hamada teaches compressed video data [column 5, lines 4-8].

As to claim 13, Hamada teaches compressed audio data [column 5, lines 4-8].

As to claim 14, Hamada teaches compressed video data and compressed audio data [column 5, lines 4-8].

As to claim 15, Hamada teaches a method of descrambling a packetized digital data stream, comprising:

> receiving a data packet stream comprising a plurality of data packets (i.e. Receiver 14 receives the dynamically encrypted stream of data at a data demultiplexer 30, which again assumes that the encryption key or encryption parameters have been multiplexed into the stream. Output from demultiplexer 30 is the encryption key and/or parameters, as well as the encrypted MPEG stream. This data is forwarded to a decryption unit 32 which then decrypts the data using the encryption information and provides an unencrypted MPEG stream to a conventional MPEG decoder 34.) [column 6 line 66 to column 7 line 7]; and
>
> descrambling (i.e. Receiver 14 receives the dynamically encrypted stream of data at a data demultiplexer 30, which again assumes that the encryption key or encryption parameters have been multiplexed into the stream. Output from demultiplexer 30 is the encryption key and/or parameters, as well as the encrypted MPEG stream. This data is forwarded to a decryption unit 32 which then decrypts the data using the encryption information and provides an unencrypted MPEG stream to a conventional MPEG decoder 34.) [column 6 line 66 to column 7 line 7] a scrambled central portion of a partially scrambled data (i.e. These parameters imply the following. The unit which will be encrypted is the picture slice. One fourth of the slices (256/1024) (i.e., every fourth slice) will be encrypted. Further, the first slice will be unencrypted; encryption will begin with the second slice (delay of 1) and continue with every fourth slice thereafter. The encryption key,

after having been initialized, will be updated at the start of every sixteenth picture (key update frequency).) [column 6, lines 18-24];

wherein the partially scrambled data payload is comprised of the scrambled central portion surrounded on both sides by an unscrambled portion (i.e. Sender 12 includes an encryption unit 20 which (in this example) receives as inputs an encryption key from a dynamic key generator 22, and the unencrypted, but encoded MPEG data stream. Any conventional encryption technique can be employed within encryption unit 20, provided that the encryption can be modified dynamically as presented herein by changing an encryption key or one or more other encryption parameters as discussed above. Output from encryption unit 20 is an encrypted MPEG stream. In this example, the encrypted MPEG stream is fed to a data multiplexer 24 which multiplexes into the stream the encryption key employed to encrypt the stream and the encryption parameters employed by the encryption unit. Data multiplexer 24 is optional since the encryption key and encryption parameters could be forwarded independent from the encrypted stream of data, for example, on a dedicated line (not shown) to the receiver 14.) [column 6, lines 49-65].

Hamada does not teach descrambling every nth packet, where n is an integer greater than 1, leaving remaining ones of the plurality of data packets as received.

Norr teaches descrambling every nth packet, where n is an integer greater than 1, leaving remaining ones of the plurality of data packets as received [column 4, lines 29-62].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hamada so that only the central portion of every nth packet, where n was an integer greater than 1, would have been decrypted and the leaving the remaining ones.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hamada by the teaching of Norr because it helps avoid unnecessary downloading of information already transmitted via broadcast airwaves, while also ensuring that copyright owners and service providers receive appropriate payments [column 2, lines 40-49].

As to claim 17, Hamada teaches an apparatus for scrambling a packetized digital data stream, comprising:

> means for producing a data packet stream comprising a plurality of data packets (i.e. Receiver 14 receives the dynamically encrypted stream of data at a data demultiplexer 30, which again assumes that the encryption key or encryption parameters have been multiplexed into the stream. Output from demultiplexer 30 is the encryption key and/or parameters, as well as the encrypted MPEG stream. This data is forwarded to a decryption unit 32 which then decrypts the data using the encryption information and provides an unencrypted MPEG stream to a conventional MPEG decoder 34.) [column 6 line 66 to column 7 line 7]; and
>
> means for scrambling a central portion of a data payload to produce a partially scrambled data payload (i.e. These parameters imply the following. The unit which will be encrypted is the picture slice. One fourth of the slices

(256/1024) (i.e., every fourth slice) will be encrypted. Further, the first slice will be unencrypted; encryption will begin with the second slice (delay of 1) and continue with every fourth slice thereafter. The encryption key, after having been initialized, will be updated at the start of every sixteenth picture (key update frequency).) [column 6, lines 18-24];

wherein the partially scrambled data payload comprised of the scrambled central portion (i.e. Sender 12 includes an encryption unit 20 which (in this example) receives as inputs an encryption key from a dynamic key generator 22, and the unencrypted, but encoded MPEG data stream. Any conventional encryption technique can be employed within encryption unit 20, provided that the encryption can be modified dynamically as presented herein by changing an encryption key or one or more other encryption parameters as discussed above. Output from encryption unit 20 is an encrypted MPEG stream. In this example, the encrypted MPEG stream is fed to a data multiplexer 24 which multiplexes into the stream the encryption key employed to encrypt the stream and the encryption parameters employed by the encryption unit. Data multiplexer 24 is optional since the encryption key and encryption parameters could be forwarded independent from the encrypted stream of data, for example, on a dedicated line (not shown) to the receiver 14.) [column 6, lines 49-65].

Hamada does not teach a receiver to receive a packet of a digital data stream wherein only some of a plurality of data packets within the digital data stream are scrambled.

Norr teaches selectively encrypting some of the packets [column 4, lines 29-62].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hamada so that the packets containing the premium channels would have only been encrypted. The packets would have included a header portion and a data payload. The data payload would have included a scrambled central portion and an unscrambled portion. A descrambler would have descrambled the scrambled central portion of the data payload of the packet. The header portion would have been entirely unscrambled.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hamada by the teaching of Norr because it helps avoid unnecessary downloading of information already transmitted via broadcast airwaves, while also ensuring that copyright owners and service providers receive appropriate payments [column 2, lines 40-49].

As to claim 19, Hamada teaches an apparatus for scrambling a packetized digital data stream, comprising: producing a data packet stream comprising:

> means for producing a data packet stream comprising a plurality of data packets (i.e. Receiver 14 receives the dynamically encrypted stream of data at a data demultiplexer 30, which again assumes that the encryption key or encryption parameters have been multiplexed into the stream. Output from demultiplexer 30 is the encryption key and/or parameters, as well as the encrypted MPEG stream. This data is forwarded to a decryption unit 32 which then decrypts the data using

the encryption information and provides an unencrypted MPEG stream to a conventional MPEG decoder 34.) [column 6 line 66 to column 7 line 7]; and

means for scrambling a central portion of a data payload to produce a partially scrambled data payload (i.e. These parameters imply the following. The unit which will be encrypted is the picture slice. One fourth of the slices (256/1024) (i.e., every fourth slice) will be encrypted. Further, the first slice will be unencrypted; encryption will begin with the second slice (delay of 1) and continue with every fourth slice thereafter. The encryption key, after having been initialized, will be updated at the start of every sixteenth picture (key update frequency).) [column 6, lines 18-24];

wherein the partially scrambled data payload is comprised of the scrambled central portion surrounded on both sides by an unscrambled portion (i.e. Sender 12 includes an encryption unit 20 which (in this example) receives as inputs an encryption key from a dynamic key generator 22, and the unencrypted, but encoded MPEG data stream. Any conventional encryption technique can be employed within encryption unit 20, provided that the encryption can be modified dynamically as presented herein by changing an encryption key or one or more other encryption parameters as discussed above. Output from encryption unit 20 is an encrypted MPEG stream. In this example, the encrypted MPEG stream is fed to a data multiplexer 24 which multiplexes into the stream the encryption key employed to encrypt the stream and the encryption

> parameters employed by the encryption unit. Data multiplexer 24 is optional since the encryption key and encryption parameters could be forwarded independent from the encrypted stream of data, for example, on a dedicated line (not shown) to the receiver 14.) [column 6, lines 49-65].

Hamada does not teach a receiver to receive a packet of a digital data stream wherein only some of a plurality of data packets within the digital data stream are scrambled.

Norr teaches selectively encrypting some of the packets [column 4, lines 29-62].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hamada so that the packets containing the premium channels would have only been encrypted. The packets would have included a header portion and a data payload. The data payload would have included a scrambled central portion and an unscrambled portion. A descrambler would have descrambled the scrambled central portion of the data payload of the packet. The header portion would have been entirely unscrambled.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hamada by the teaching of Norr because it helps avoid unnecessary downloading of information already transmitted via broadcast airwaves, while also ensuring that copyright owners and service providers receive appropriate payments [column 2, lines 40-49].

As to claim 21, Hamada teaches an apparatus for descrambling a packetized digital data stream, comprising:

means for receiving a data packet stream comprising a plurality of data packets (i.e. Receiver 14 receives the dynamically encrypted stream of data at a data demultiplexer 30, which again assumes that the encryption key or encryption parameters have been multiplexed into the stream. Output from demultiplexer 30 is the encryption key and/or parameters, as well as the encrypted MPEG stream. This data is forwarded to a decryption unit 32 which then decrypts the data using the encryption information and provides an unencrypted MPEG stream to a conventional MPEG decoder 34.) [column 6 line 66 to column 7 line 7]; and

means for descrambling (i.e. Receiver 14 receives the dynamically encrypted stream of data at a data demultiplexer 30, which again assumes that the encryption key or encryption parameters have been multiplexed into the stream. Output from demultiplexer 30 is the encryption key and/or parameters, as well as the encrypted MPEG stream. This data is forwarded to a decryption unit 32 which then decrypts the data using the encryption information and provides an unencrypted MPEG stream to a conventional MPEG decoder 34.) [column 6 line 66 to column 7 line 7] a central portion of a partially scrambled data payload of the data packet stream where n is an integer greater than 1 [column 10, lines 18-24];

wherein the partially scrambled data payload is comprised of the scrambled central portion surrounded on both sides by an unscrambled

> portion (i.e. Sender 12 includes an encryption unit 20 which (in this example) receives as inputs an encryption key from a dynamic key generator 22, and the unencrypted, but encoded MPEG data stream. Any conventional encryption technique can be employed within encryption unit 20, provided that the encryption can be modified dynamically as presented herein by changing an encryption key or one or more other encryption parameters as discussed above. Output from encryption unit 20 is an encrypted MPEG stream. In this example, the encrypted MPEG stream is fed to a data multiplexer 24 which multiplexes into the stream the encryption key employed to encrypt the stream and the encryption parameters employed by the encryption unit. Data multiplexer 24 is optional since the encryption key and encryption parameters could be forwarded independent from the encrypted stream of data, for example, on a dedicated line (not shown) to the receiver 14.) [column 6, lines 49-65].

Hamada does not teach descrambling every nth packet, where n is an integer greater than 1, leaving remaining ones of the plurality of data packets as received.

Norr teaches descrambling every nth packet, where n is an integer greater than 1, leaving remaining ones of the plurality of data packets as received [column 4, lines 29-62].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hamada so that only the central portion of every nth packet, where n was an integer greater than 1, would have been decrypted and the leaving the remaining ones.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hamada by the teaching of Norr because it helps avoid unnecessary downloading of information already transmitted via broadcast airwaves, while also ensuring that copyright owners and service providers receive appropriate payments [column 2, lines 40-49].

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2131
/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131